UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF WEST VIRGINIA

IN THE MATTER OF THE SEARCH OF: **A 2012 WHITE JEEP GRAND CHEROKEE WITH WEST VIRGINIA LICENSE TAG 53T507, VIN: 1C4RJFAT2CC204303**	**No.** 1:21-mj-24

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Riley Palmertree, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as **205 BLUE RIDGE LANE MORGANTOWN, WV 26508,** hereinafter "**PREMISES," 708 BEECHURST AVENUE, MORGANTOWN, WV 26505, hereinafter "BUSINESS,"** and **2012 WHITE JEEP GRAND CHEROKEE WITH WEST VIRGINIA LICENSE TAG 53T507 and VIN: 1C4RJFAT2CC204303,** hereinafter **"VEHICLE"**[1] further described in Attachment A, for the things described in Attachment B.

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"). I have been in this position since since May 2017. I am currently assigned to the FBI Washington Field Office ("WFO") in Washington, D.C. I am currently assigned to the Violent Crimes Task Force Squad CR-2, which focuses on the Washington, D.C. metropolitan area. I have investigated violent

[1] The VEHICLE appears to have an expired registration and lists the owner as George TANIOS with an address of 120 Putnam Street, Morgantown, West Virginia. Your affiant believes this may have been a previous residence of TANIOS and as of March 5, 2021 appears to be vacant.

crimes since approximately October of 2017. As part of my duties, I have investigated homicides, bank robberies, carjackings, kidnappings, fugitive cases, and other crimes of violence. During these investigations, I have employed a variety of investigative techniques including preparing and executing search and arrest warrants that have led to seizures of contraband.

2. I am one of the investigators assigned to an ongoing investigation by the FBI, United States Capitol Police ("USCP"), Metropolitan Police Department ("MPD"), and other law enforcement agencies, of riots and civil disorder that occurred on January 6, 2021, in and around the United States Capitol grounds. Since I became involved in this investigation on January 6, 2021, I have conducted interviews, reviewed public tips, reviewed publicly available photos and video, and reviewed relevant documents, among other things.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that violations of 18 U.S.C. §§ 372, 111(a), 111(b), 2, 231(a)(3), 1512(c)(2), 1752(a)(1), (2) & (4), (b)(1)(A), and 40 U.S.C. § 5104(e)(2), have been committed by multiple identified and unidentified individuals. There is also probable cause to search the information described in Attachment A for evidence relating to these crimes as further described in Attachment B.

5. As a federal agent, I am authorized to investigate violations of laws of the United States, and as a law enforcement officer, I am authorized to execute warrants issued under the authority of the United States.

6. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter.

7. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that violations of 18 U.S.C. § 372 (Conspiracy to injure an officer), 18 U.S.C. §§ 111 (a) and (b) (Assaulting an Officer of the United States with a deadly or dangerous weapon); 18 U.S.C. § 2 (Aiding and Abetting), 18 U.S.C. § 231 (Civil Disorder); 18 U.S.C. § 1512(c)(2) (Obstruction of an Official Proceeding); 18 U.S.C. § 1752(a) and (b) (Physical violence on restricted grounds, while carrying dangerous weapon, and resulting in significant bodily injury); 40 U.S.C. § 5104(e)(2)(F) (Violent Entry, Disorderly Conduct and act of physical violence on Capitol Grounds) (the "Target Offenses") have been committed by JULIAN ELIE KHATER and GEORGE PIERRE TANIOS ("the Subjects") and other identified and unidentified persons, including others who may have been aided and abetted by, or conspiring with, the Subjects, as well as others observed by the Subjects. There is also probable cause to search the PREMISES, BUSINESS, and VEHICLE, further described in Attachment A, for the things described in Attachment B.

PROBABLE CAUSE

Background – The U.S. Capitol on January 6, 2021

8. The United States Capitol Police ("USCP"), the FBI, and assisting law enforcement agencies are investigating a riot and related offenses that occurred at the United States Capitol Building, located at 1 First Street, NW, Washington, D.C., 20510 at latitude 38.88997 and longitude -77.00906 on January 6, 2021.

9. At the U.S. Capitol, the building itself has 540 rooms covering 175,170 square feet of ground, roughly four acres. The building is 751 feet long (roughly 228 meters) from north to south and 350 feet wide (106 meters) at its widest point. The U.S. Capitol Visitor Center is 580,000 square feet and is located underground on the east side of the Capitol. On the west side of the Capitol building is the West Front, which includes the inaugural stage scaffolding, a variety of open concrete spaces, a fountain surrounded by a walkway, two broad staircases, and multiple terraces at each floor. On the East Front are three staircases, porticos on both the House and Senate side, and two large skylights into the Visitor's Center surrounded by a concrete parkway. All of this area was barricaded and off limits to the public on January 6, 2021.

10. The U.S. Capitol is secured 24 hours a day by USCP. Restrictions around the U.S. Capitol include permanent and temporary security barriers and posts manned by USCP. Only authorized people with appropriate identification are allowed access inside the U.S. Capitol.

11. On January 6, 2021, a joint session of the United States Congress was scheduled to convene at the U.S. Capitol to certify the vote count of the Electoral College of the 2020

Presidential Election, which took place on November 3, 2020 ("Certification"). The exterior plaza of the U.S. Capitol was closed to members of the public.

12. A crowd began to assemble near the Capitol around 12:30 p.m. Eastern Standard Time (EST), and at about 12:50 p.m., known and unknown individuals broke through the police lines, toppled the outside barricades protecting the U.S. Capitol, and pushed past USCP and supporting law enforcement officers there to protect the U.S. Capitol.

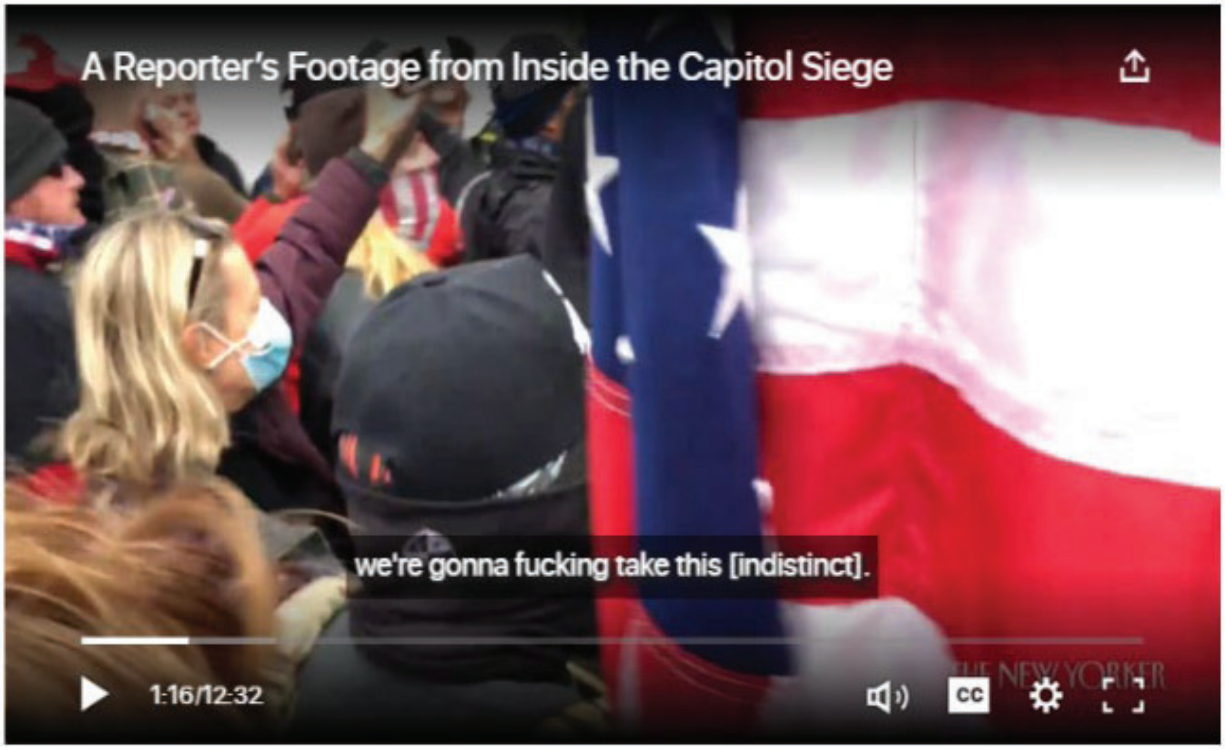
13. The joint session began at approximately 1:00 p.m. in the House Chamber.

14. At approximately 1:30 p.m., the House and Senate adjourned to separate chambers to resolve a particular objection. Vice President Mike Pence was present and presiding, first in the joint session, and then in the Senate chamber. Also around this time, USCP ordered Congressional staff to evacuate the House Cannon Office Building and the Library of Congress James Madison Memorial Building, in part because of a suspicious package found nearby. Pipe bombs were later found near both the Democratic National Committee and Republican National Committee headquarters.

15. As the proceedings continued in both the House and the Senate, USCP attempted to keep the crowd away from the Capitol building and the proceedings underway inside. Media reporting showed a group of individuals outside of the Capitol chanting, "Hang Mike Pence." I know from this investigation that some individuals believed that Vice President Pence possessed the ability to prevent the certification of the presidential election and that his failure to do so made him a traitor.

16. At approximately 2:00 p.m., some people in the crowd forced their way through, up, and over additional barricades and law enforcement. The crowd advanced to the exterior façade of the building. The crowd was not lawfully authorized to enter or remain in the building and, prior to entering the building, no members of the crowd submitted to security screenings or weapons checks by USCP officers or other authorized security officials. At such time, the certification proceedings were still underway and the exterior doors and windows of the U.S. Capitol were locked or otherwise secured. Members of law enforcement attempted to maintain order and keep the crowd from entering the Capitol.

17. At about 2:10 p.m., individuals in the crowd forced entry into the U.S. Capitol, including by breaking windows and by assaulting members of law enforcement, as others in the crowd encouraged and assisted those acts. Publicly available video footage shows an unknown individual saying to a crowd outside the Capitol building, "We're gonna fucking take this," which your affiant believes was a reference to "taking" the U.S. Capitol.



18. Shortly thereafter, at approximately 2:20 p.m. members of the United States House of Representatives and United States Senate, including the President of the Senate, Vice President Mike Pence, were instructed to—and did—evacuate the chambers. That is, at or about this time, USCP ordered all nearby staff, Senators, and reporters into the Senate chamber and locked it down. USCP ordered a similar lockdown in the House chamber. As rioters attempted to break into the House chamber, by breaking the windows on the chamber door, law enforcement were forced to draw their weapons to protect the victims sheltering inside.

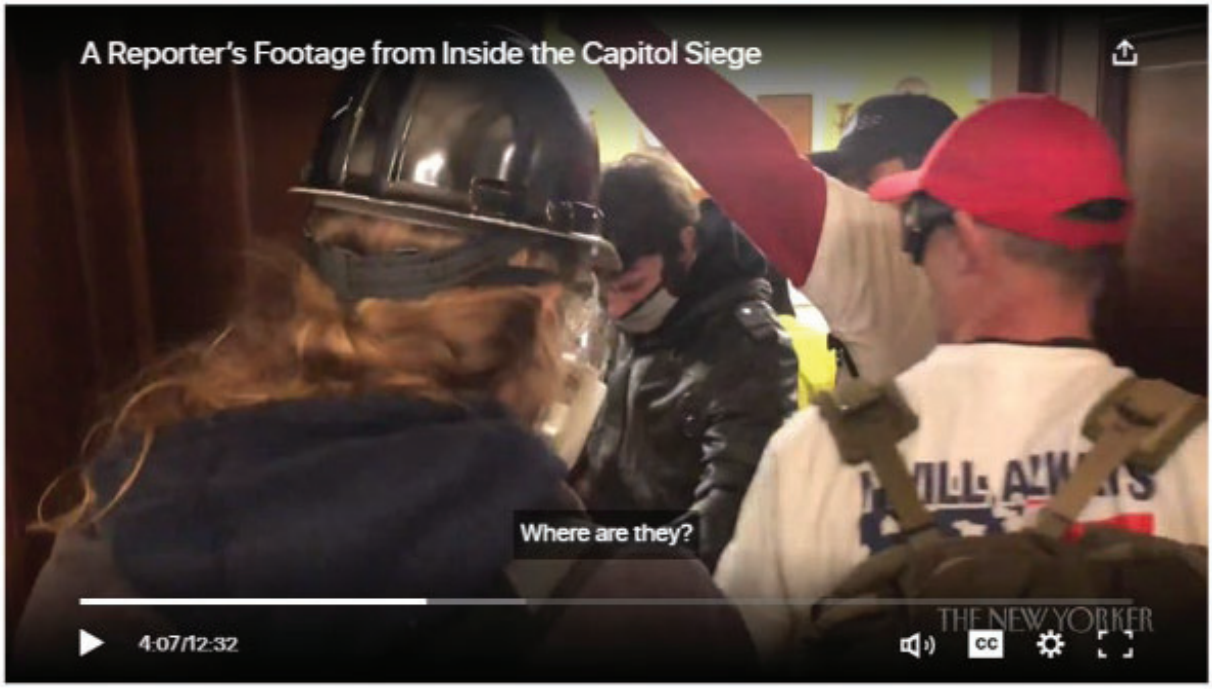
19. At approximately 2:30 p.m., known and unknown subjects broke windows and pushed past USCP and supporting law enforcement officers forcing their way into the U.S. Capitol

on both the west side and the east side of the building. Once inside, the subjects broke windows and doors, destroyed property, stole property, and assaulted federal police officers. Many of the federal police officers were injured and several were admitted to the hospital. The subjects also confronted and terrorized members of Congress, Congressional staff, and the media. The subjects carried weapons including tire irons, sledgehammers, bear spray, and tasers. They also took police equipment from overrun police including shields and police batons. At least one of the subjects carried a handgun with an extended magazine. These actions by the unknown individuals resulted in the disruption and ultimate delay of the vote Certification.

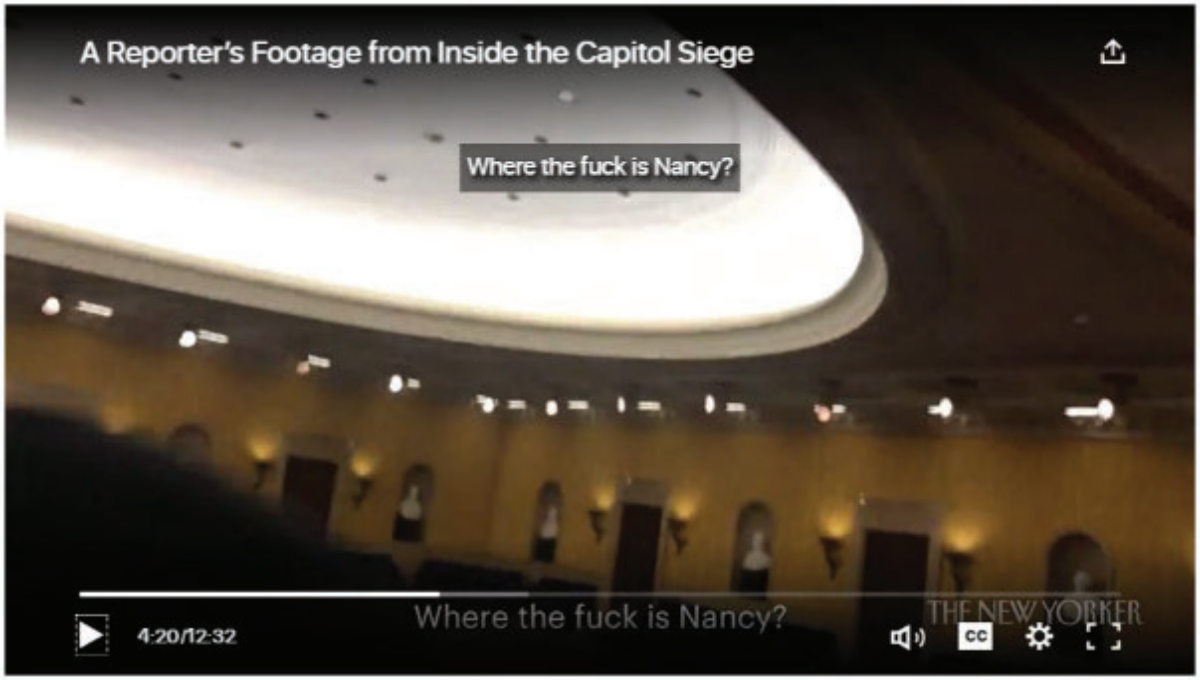
20. Also at approximately 2:30 p.m., as subjects reached the rear door of the House Chamber, USCP ordered the evacuation of lawmakers, Vice President Mike Pence, and president pro tempore of the Senate, Charles Grassley, for their safety.

21. At around 2:45 p.m., subjects broke into the office of House Speaker Nancy Pelosi. At about the same time, one subject was shot and killed while attempting to break into the House chamber through the broken windows.

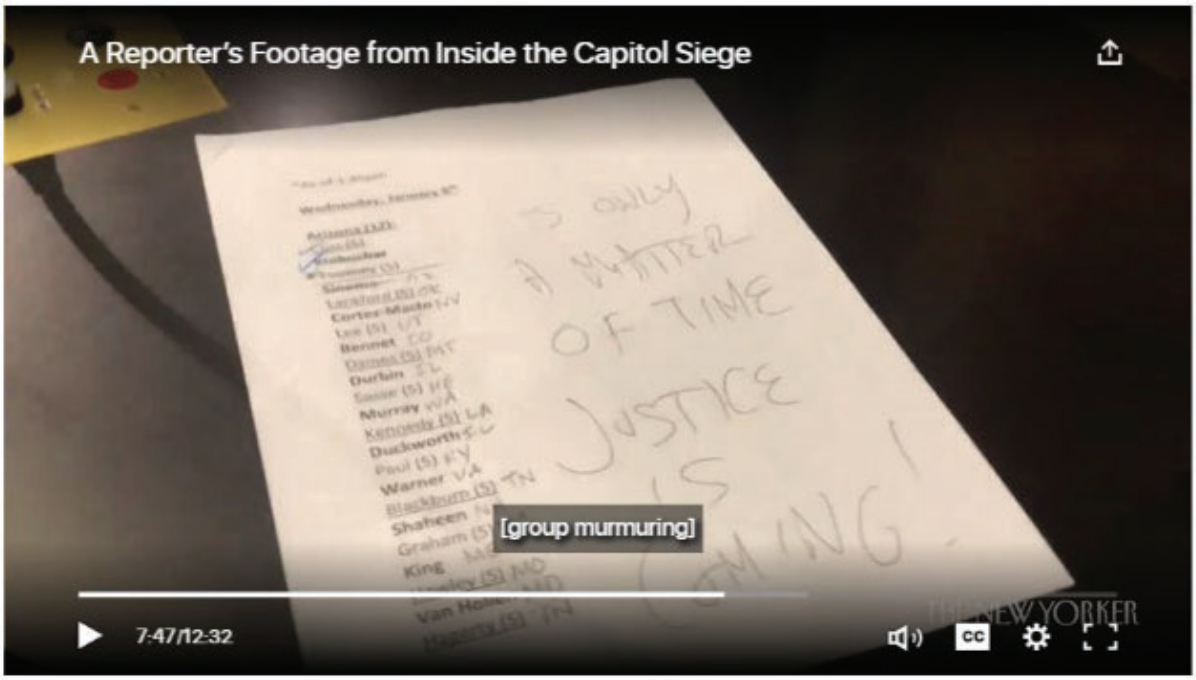
22. At around 2:47 p.m., subjects broke into the United States Senate Chamber. Publicly available video shows an individual asking, "Where are they?" as they opened up the door to the Senate Chamber. Based upon the context, law enforcement believes that the word "they" is in reference to members of Congress.



23. After subjects forced entry into the Senate Chamber, publicly available video shows that an individual asked, "Where the fuck is Nancy?" Based upon other comments and the context, law enforcement believes that the "Nancy" being referenced was the Speaker of the House of Representatives, Nancy Pelosi.



24. A subject left a note on the podium on the floor of the Senate Chamber. This note, captured by the filming reporter, stated "It's Only A Matter of Time Justice is Coming."



25. During the time when the subjects were inside the Capitol building, multiple subjects were observed inside the U.S. Capitol wearing what appears to be, based upon my training and experience, tactical vests and carrying flex cuffs. Based upon my knowledge, training, and experience, I know that flex cuffs are a manner of restraint that are designed to be carried in situations where a large number of individuals were expected to be taken into custody.

26. At around 2:48 p.m., DC Mayor Muriel Bowser announced a citywide curfew beginning at 6:00 p.m.

27. At about 3:25 p.m., law enforcement officers cleared the Senate floor.

28. Between 3:25 and around 6:30 p.m., law enforcement was able to clear the U.S. Capitol of all of the subjects.

29. Based on these events, all proceedings of the United States Congress, including the joint session, were effectively suspended until shortly after 8:00 p.m. the same day. In light of the dangerous circumstances caused by the unlawful entry to the U.S. Capitol, including the danger posed by individuals who had entered the U.S. Capitol without any security screening or weapons check, Congressional proceedings could not resume until after every unauthorized occupant had left the U.S. Capitol, and the building had been confirmed secured. The proceedings resumed at approximately 8:00 pm after the building had been secured. Vice President Pence remained in the United States Capitol from the time he was evacuated from the Senate Chamber until the session resumed.

30. Beginning around 8:00 p.m., the Senate resumed work on the Certification.

31. Beginning around 9:00 p.m., the House resumed work on the Certification.

32. Both chambers of Congress met and worked on the Certification within the Capitol building until approximately 3:00 a.m. on January 7, 2021.

33. During national news coverage of the aforementioned events, video footage which appeared to be captured on mobile devices of persons present on the scene depicted evidence of violations of local and federal law, including scores of individuals inside the U.S. Capitol building without authority to be there.

34. Based on my training and experience, I know that it is common for individuals to carry and use their cell phones during large gatherings, such as the gathering that occurred in the area of the U.S. Capitol on January 6, 2021. Such phones are typically carried at such gatherings to allow individuals to capture photographs and video footage of the gatherings, to communicate with other individuals about the gatherings, to coordinate with other participants at the gatherings, and to post on social media and digital forums about the gatherings.

35. Many subjects seen on news footage in the area of the U.S. Capitol are using a cell phone in some capacity. It appears some subjects were recording the events occurring in and around the U.S. Capitol and others appear to be taking photos, to include photos and video of themselves after breaking into the U.S. Capitol itself, including photos of themselves damaging and stealing property. As reported in the news media, others inside and immediately outside the U.S. Capitol live-streamed their activities, including those described above as well as statements about these activities.

36. Photos below, available on various publicly available news, social media, and other media show some of the subjects within the U.S. Capitol during the riot. In several of these photos,

the individuals who broke into the U.S. Capitol can be seen holding and using cell phones, including to take pictures and/or videos:

[2]

[2] https://losangeles.cbslocal.com/2021/01/06/congresswoman-capitol-building-takeover-an-attempted-coup/

 [3]

[3] https://www.businessinsider.com/republicans-objecting-to-electoral-votes-in-congress-live-updates-2021-1.

 [4]

Facts Specific to PREMISES, BUSINESS, and VEHICLE

SUBJECTS Assault on Federal Officers

37. At approximately 1:00 p.m., a crowd of violent rioters had assembled on the Lower West Terrace. U. S. Capitol Police had formed a line of bike racks extending from the North end of the Lower West Terrace to the South end, to act as a barrier against the crowd. Officers were standing watch behind this line and fending off repeated attempts by the rioters to pull on the bike racks, either with their hands or with ropes and straps.

38. In reviewing surveillance footage of this incident, your affiant observed the SUBJECTS, JULIAN ELIE KHATER and GEORGE PIERRE TANIOS, working together to

[4]https://www.thv11.com/article/news/arkansas-man-storms-capitol-pelosi/91-41abde60-a390-4a9e-b5f3-d80b0b96141e

assault law enforcement officers with an unknown chemical substance by spraying officers directly in the face and eyes. Your affiant further observed these SUBJECTS appeared to time the deployment of chemical substances to coincide with other rioters' efforts to forcibly remove the bike rack barriers that were preventing the rioters from moving closer to the Capitol building.

39. Surveillance footage shows that at 2:09 p.m., TANIOS can be seen walking from the south grassy area toward the Lower West Terrace. KHATER can be seen walking behind TANIOS. KHATER is wearing a beanie with a pom-pom on top, a dark jacket, and has a beard. TANIOS is wearing a red hat, black backpack, dark hooded sweatshirt, and has a beard. At 2:14 p.m., TANIOS and KHATER can be seen engaging each other in animated conversation while they are standing together.

40. During the investigation, law enforcement discovered open source media video of the incident from January 6, 2021. On the video, KHATER is seen making his way towards TANIOS. KHATER then states, "Give me that bear shit," and reaches into the backpack on TANIOS' back. TANIOS then states, "Hold on, hold on, not yet, not yet… its still early." KHATER is then seen emphatically telling TANIOS, "They just fucking sprayed me," and KHATER is seen holding a white can with a black top that appears to be a can of chemical spray. See Figure One, below.

Figure One

41. This verbal exchange between KHATER and TANIOS, together with KHATER's retrieval of the spray can from TANIOS, reveals that the two were working in concert and had a plan to use the toxic spray against law enforcement.

42. On the video, KHATER continues to talk animatedly with TANIOS. At approximately 2:20 p.m., KHATER walks through the crowd to within a few steps of the bike rack barrier. KHATER is standing directly across from a line of law enforcement officers to include U.S. Capitol Police ("USCP") Officers B. Sicknick and C. Edwards, and Metropolitan Police Department ("MPD") Officer D. Chapman, who was equipped with a functioning body worn camera ("BWC") device.

43. Officer Chapman's BWC shows that at 2:23 p.m., the rioters begin pulling on a bike rack to Chapman's left, using ropes and their hands to pull the rack away. Seconds later, KHATER is observed with his right arm up high in the air, appearing to be holding a canister in his right hand and aiming it in the officers' direction while moving his right arm from side to side. Officer Chapman's BWC confirms that KHATER was standing only five to eight feet away from the officers. *See* Figure Two, below.

Figure Two

44. In reviewing the surveillance footage and BWC video, your affiant observes that Officers Sicknick, Edwards and Chapman, who are standing within a few feet of KHATER, all react, one by one, to something striking them in the face. The officers immediately retreat from the line, bring their hands to their faces and rush to find water to wash out their eyes, as described

in further detail below and as captured in the following screen shots. *See* Figures Three and Four, below.

Figure Three

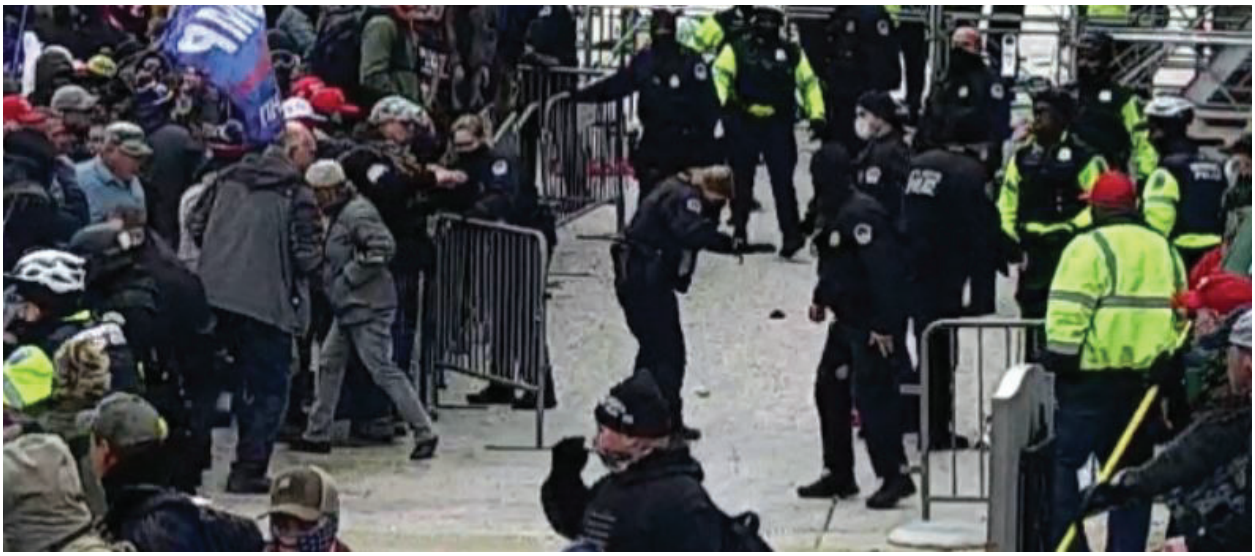


Figure Four

45. At 2:23 p.m., on the surveillance footage, KHATER is again observed raising his arm and continues to spray in the direction of law enforcement officers. MPD Lt. Bagshaw notices these actions and approaches KHATER. At 2:23 p.m., Lt. Bagshaw then sprays KHATER, as observed on both surveillance footage and Lt. Bagshaw's BWC. *See* Figure Five, below.

Figure Five

Injuries to Officers

46. Officers Sicknick, Edwards, and Chapman suffered injuries as a result of being sprayed in the face with an unknown substance by KHATER. The officers were temporary blinded by the substance, were temporary disabled from performing their duties and needed medical attention and assistance from fellow officers. They were initially treated with water in an effort to wash out the unknown substance from their eyes and on their face. All three officers were incapacitated and unable to perform their duties for at least 20 minutes or longer while they recovered from the spray. Officer Edwards reported lasting injuries underneath her eyes, including scabbing that remained on her face for weeks. Officers Edwards and Chapman also described the spray to their face as a substance as strong as, if not stronger than, any version of pepper spray they had been exposed to during their training as law enforcement officers. Officer Sicknick reported to his supervisors and colleagues that he had been sprayed in the face with a substance.

Identification of the SUBJECTS

47. Based on the above surveillance footage, law enforcement prepared flyers with photographs of KHATER and TANIOS, which were published along with other individuals involved in the violence at the U.S. Capitol on January 6, 2021. SUBJECT KHATER was listed as subject number 190. SUBJECT TANIOS was listed as subject number 254. A tipster to the FBI provided information that TANIOS and KHATER knew each other and grew up together in New Jersey.

a. **Identification of JULIAN KHATER**

48. During the investigation, law enforcement received information from a tipster regarding subject 190. The tipster relayed that the subject was the same person who owned a Linkedin page belonging to JULIAN KHATER.

49. Based on a review of this Linkedin page, law enforcement identified and spoke by telephone to W-1. W-1 stated IT was a former work colleague of KHATER. Your affiant provided W-1 an image of subject 190, and W-1 positively identified the individual as "Julian" and stated IT was "100% sure" the individual was "Julian," whom IT knew from working together at a food establishment in State College, Pennsylvania. W-1 saw KHATER approximately three to four times per week from July 2019 to November 2019, and last saw KHATER in November 2019. W-1 did not immediately remember KHATER's last name, but looked up an old work document that listed Julian's last name as KHATER.

b. Identification of GEORGE TANIOS

49. During the investigation, law enforcement received two tips that included a photo posted on social media of TANIOS at the Capitol on January 6, 2021. *See* Figure Six, below.

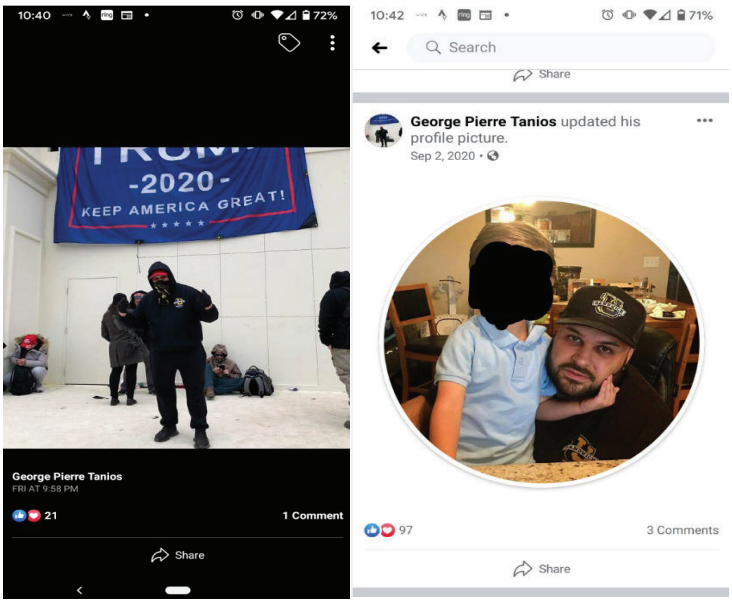


Figure Six

50. The tipsters stated that the photo was from a Facebook page belonging to an individual named "GEORGE PIERRE TANIOS" and confirmed that TANIOS was wearing clothing with the insignia of "Sandwich University" in both his profile picture and his picture at the Capitol. Your affiant notes that the hooded sweatshirt that TANIOS is wearing in the Capitol picture appears identical to the sweatshirt worn by TANIOS in the surveillance video, as seen below in Figure Seven:

Figure Seven

51. Another tipster reported to law enforcement that BOLO 254 looked "very close" to George Pierre Tanios from New Jersey, and that TANIOS had bragged about going to the insurrection at the Capitol on Facebook. The tipster also indicated that TANIOS owns the "Fat Sandwich" restaurant.

52. Utilizing a public records database, law enforcement located a GEORGE PIERRE TANIOS, born in New Brunswick, NJ, and found the below photograph (Figure Eight) of TANIOS at his business in Morgantown, West Virginia.

Figure Eight

53. TANIOS is wearing a shirt with a Sandwich University logo identical to the clothing seen in both his social media post and the Capitol surveillance footage. A search of social media also revealed a profile of an individual named "George Pierre Tanios," with the username "kingofthefatsandwich."

54. Law enforcement interviewed W-2 and provided two images of TANIOS for W-2 to review. Upon viewing the two images of TANIOS, W-2 positively identified the individual in the photos as TANIOS. W-2 stated that IT was "100%" sure the individual in one photo was TANIOS, and "pretty sure" the individual in the second photo was TANIOS. W-2 has known TANIOS for 15 years, and they are former business partners. W-2 reported that IT was in a legal dispute with TANIOS where TANIOS reportedly embezzled $435,000 from their former business.

2. NEXUS TO PREMISES

55. The PREMISES is located at 205 BLUE RIDGE LANE, MORGANTOWN, WEST VIRGINIA, 26508. The premises is a beige townhouse with a white garage. The number 205 appears on the front door. Accurint records reveal that TANIOS resides at the PREMISES. On March 7, 2021, at approximately 11:03 a.m., the VEHICLE was parked in the driveway of the PREMISES. On March 8, 2021, at approximately 10:00 a.m., law enforcement observed the VEHICLE parked in the driveway of the PREMISES. Also, on March 8, 2021, at approximately 2:19 p.m., law enforcement observed TANIOS exit the PREMISES, enter the VEHICLE which was parked in the driveway, and drive to the BUSINESS. TANIOS' West Virginia driver's license which was issued January 9, 2017, lists TANIOS' address as 120 Putnam Street, Morgantown, West Virginia. Your affiant believes that this is TANIOS' old address and appears to be vacant.

3. NEXUS TO BUSINESS

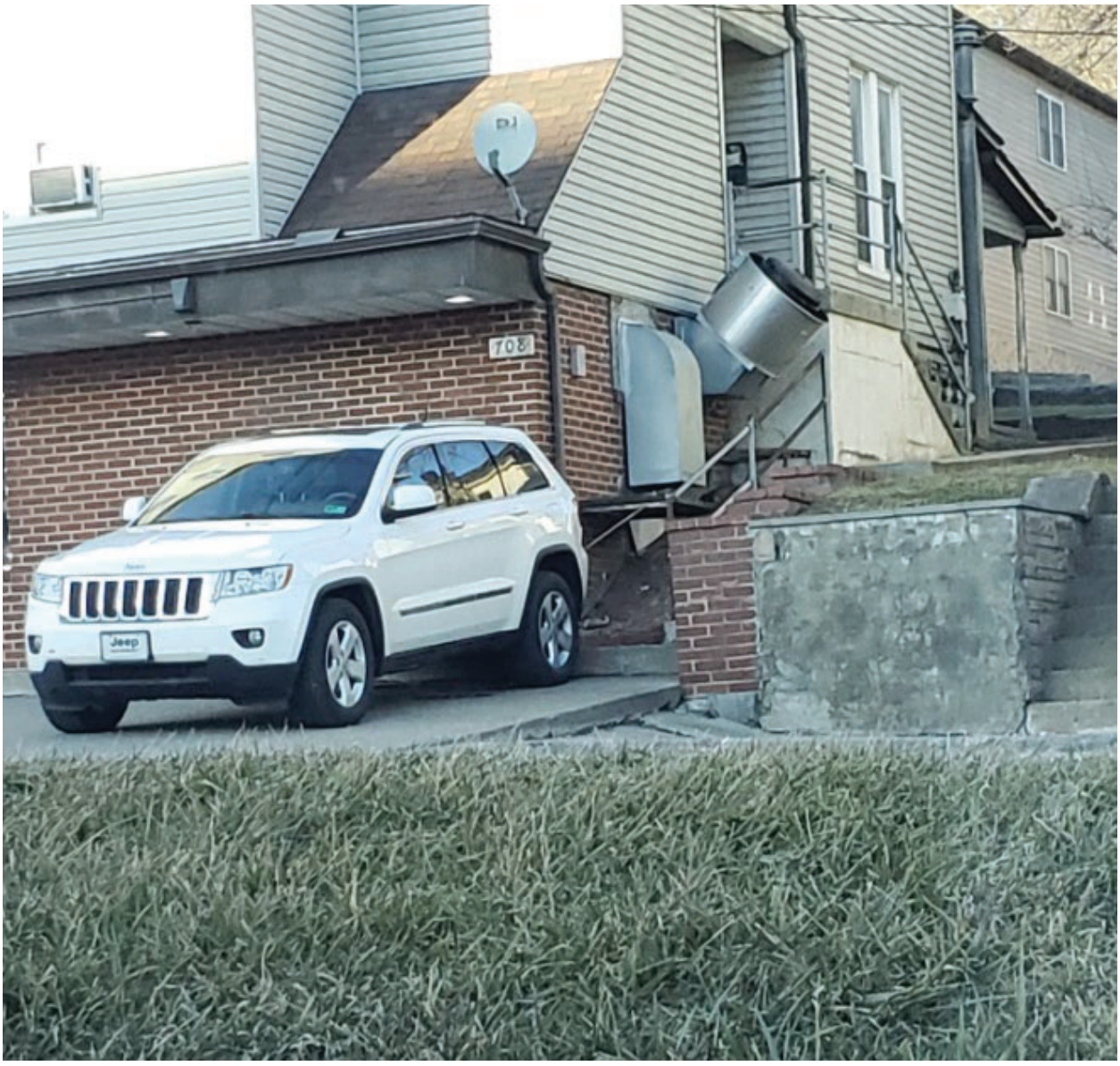
56. The BUSINESS is located at 708 Beechurst Avenue, Morgantown, West Virginia, 26505. The premises is a fast food eatery called Sandwich University. The structure appears to be a sit-down and takeout restaurant with a brick front and a sign that states Sandwich University above the front entrance door. Accurint records list TANIOS as a member, president, and chief executive officer of the BUSINESS. An open source article from March 21, 2019, shows a photograph of TANIOS and discusses the BUSINESS. The article identifies TANIOS as the general manager. On March 5, 2021, at approximately 5:25 p.m., and March 7, 2021, at approximately 7:30 a.m., law enforcement observed the VEHICLE parked outside of the BUSINESS. On March 8, 2021, at approximately 2:19 p.m., law enforcement observed TANIOS

exit the PREMISES, enter the VEHICLE in the driveway, and drive to the BUSINESS.

4. NEXUS TO VEHICLE

57. The VEHICLE is described as a 2012 white Jeep Grand Cherokee with West

Virginia license tag 53T507, VIN: 1C4RJFAT2CC204303. The VEHICLE appears to have an expired registration and lists the owner as George TANIOS with an address of 120 Putnam Street, Morgantown, West Virginia. Your affiant believes this may have been a previous residence of TANIOS. On March 5, 2021, law enforcement conducted surveillance 120 Putnam Street and appears to be vacant. On March 5, 2021, at approximately 5:25 p.m., law enforcement observed the VEHICLE parked outside of the BUSINESS, which your affiant knows is Sandwich University, owned by TANIOS. Also, on March 8, 2021, at approximately 2:19 p.m., law enforcement observed TANIOS exit the PREMISES, enter the VEHICLE which was parked in the driveway, and drive to the BUSINESS.


708
Jeep

58. Through this investigation, your affiant knows that TANIOS wore distinctive clothing, a backpack, and had had a chemical spray in his custody. Your affiant knows, based on

my training and experience, that people routinely re-wear clothing and accessories and store these items in their residences or vehicles, and in this instance likely in TANIOS' BUSINESS he is the owner of the establishment because it is restaurant clothing. Clothing and accessories consistent with those worn by TANIOS on January 6, 2021 constitute evidence of the commission of the offenses discussed herein, in that TANIOS can be visually identified as the individual in the photos and videos discussed above, in part through the distinct attire including clothing (with BUSINESS logo), and accessories worn that day. Additionally, I also know, based on my training and experience, that cell phones are expensive, and people routinely retain their cell phones for many months or years.

59. Additionally, through the investigation, your affiant knows that TANIOS and KHATER utilized cellular telephones to communicated on January 6, 2021 at the U.S. Capitol. Law enforcement database shows TANIOS associated with telephone number (304) 777-3321, the subscriber is AT&T. Law enforcement is awaiting additional information from AT&T telephones associated with TANIOS and about telephone number (304) 777-3321. Verizon records show that KHATER is associated with telephone number (732) 439-1927. Based on a review U.S. Capitol Police video footage (see image below), KHATER is seen making or answering a telephone call at 2:42 p.m. on January 6, 2021, and TANIOS does not appear to be physically near KHATER at that time. The call lasts approximately 20 seconds. A review of the Verizon records for the telephone associated with KHATER, (732) 439-1927, reveals that (732) 439-1927 was on a 21-second call with (304) 777-3321 at that time.

60. There is evidence that TANIOS and KHATER were in possession of cellular telephones while at the U.S. Capitol on January 6, 2021. In addition, based on photos and videos of the offenses that date, numerous persons committing the Target Offenses possessed digital devices that they used to record and post photos and videos of themselves and others committing those offenses. Further, based on the investigation, numerous persons committing the Target Offenses possessed digital devices to communicate with other individuals to plan their attendance at the gatherings, to coordinate with other participants at the gatherings, and to post on social media and digital forums about the gatherings.

61. Moreover, it is well-known that virtually all adults in the United States use mobile digital devices. In a fact sheet from June 12, 2019, The Pew Research Center for Internet & Technology estimated that 96% of Americans owned at least one cellular phone, and that that same 2019 report estimated that 81% of Americans use at least one smartphone. *See* Mobile Fact Sheet, https://www.pewresearch.org/internet/fact-sheet/mobile/ (last visited Jan. 9, 2021).

62. In addition, in my training and experience, it is common for individuals to back up or preserve copies of digital media (such as photos and videos) across multiple devices to prevent loss. Indeed, some companies provide services that seamlessly sync data across devices, such as Apple devices and the Apple iCloud service. Thus, there is reason to believe that evidence of the offense that originally resided on TANIOS' cell phone may also be saved to other digital devices within his PREMISES, BUSINESS, or VEHICLE. Moreover, here, as widely reported in the news media related to this matter, many individual committing the Target Offenses kept and posted videos, photos, and commentary about their participation in these offenses, essentially bragging about their participation. Based on that, there is also probable cause to believe that evidence related to these offenses may have been transferred to and stored on digital devices beyond the particular digital device the Subject possessed during the offenses.

a. These individuals usually maintain these photographs and recordings in their possession, at their premises, or at some other safe place.

b. Those making threats to injure through interstate commerce often maintain weapons, including guns and ammunition, in secure locations such as their residences and vehicles.

63. Based on my training and experience, and on conversations I have had with other law enforcement officers, I know that some individuals who participate in activities aimed at disrupting or interfering with governmental and/or law enforcement operations have been known to use anonymizing services and/or applications capable of encrypting communications to protect their identity and communications. By using such tools, in some cases, the only way to see the content of these conversations is on the electronic device that had been used to send or receive the communications.

Technical Terms

64. Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, I know the terms described below have the following meanings or characteristics:

a. "Digital device," as used herein, includes the following three terms and their respective definitions:

1) A "computer" means an electronic, magnetic, optical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1). Computers are physical units of equipment that perform information

processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

2) "Digital storage media," as used herein, means any information storage device in which information is preserved in binary form and includes electrical, optical, and magnetic digital storage devices. Examples of digital storage media include, but are not limited to, compact disks, digital versatile disks ("DVDs"), USB flash drives, flash memory cards, and internal and external hard drives.

3) "Computer hardware" means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

b. "Wireless telephone" (or mobile telephone, or cellular telephone), a type of digital device, is a handheld wireless device used for voice and data communication at least in part through radio signals and also often through "wi-fi" networks. When communicating via radio

signals, these telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones, traditional "land line" telephones, computers, and other digital devices. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of applications and capabilities. These include, variously: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages, e-mail, and other forms of messaging; taking, sending, receiving, and storing still photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; utilizing global positioning system ("GPS") locating and tracking technology, and accessing and downloading information from the Internet.

c. A "tablet" is a mobile computer, typically larger than a wireless phone yet smaller than a notebook, that is primarily operated by touch-screen. Like wireless phones, tablets function as wireless communication devices and can be used to access the Internet or other wired or wireless devices through cellular networks, "wi-fi" networks, or otherwise. Tablets typically contain programs called applications ("apps"), which, like programs on both wireless phones, as described above, and personal computers, perform many different functions and save data associated with those functions.

d. A "GPS" navigation device, including certain wireless phones and tablets, uses the Global Positioning System (generally abbreviated "GPS") to display its current location,

and often retains records of its historical locations. Some GPS navigation devices can give a user driving or walking directions to another location, and may contain records of the addresses or locations involved in such historical navigation. The GPS consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. "Computer passwords and data security devices" means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

f. "Computer software" means digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software

is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. Internet Protocol ("IP") Address is a unique numeric address used by digital devices on the Internet. An IP address, for present purposes, looks like a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 149.101.1.32). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. The "Internet" is a global network of computers and other electronic devices that communicate with each other using numerous specified protocols. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

i. "Internet Service Providers," or "ISPs," are entities that provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet, including via telephone-based dial-up and broadband access via digital subscriber line ("DSL"), cable, dedicated circuits, fiber-optic, or satellite. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports.

Many ISPs assign each subscriber an account name, a user name or screen name, an e-mail address, an e-mail mailbox, and a personal password selected by the subscriber. By using a modem, the subscriber can establish communication with an ISP and access the Internet by using his or her account name and password.

j. A "modem" translates signals for physical transmission to and from the ISP, which then sends and receives the information to and from other computers connected to the Internet.

k. A "router" often serves as a wireless Internet access point for a single or multiple devices, and directs traffic between computers connected to a network (whether by wire or wirelessly). A router connected to the Internet collects traffic bound for the Internet from its client machines and sends out requests on their behalf. The router also distributes to the relevant client inbound traffic arriving from the Internet. A router usually retains logs for any devices using that router for Internet connectivity. Routers, in turn, are typically connected to a modem.

l. "Domain Name" means the common, easy-to-remember names associated with an IP address. For example, a domain name of "www.usdoj.gov" refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first-level, or top-level domains are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and .edu for educational organizations. Second-level names will further identify the organization, for example

usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

m. "Cache" means the text, image, and graphic files sent to and temporarily stored by a user's computer from a website accessed by the user in order to allow the user speedier access to and interaction with that website in the future.

n. "Peer to Peer file sharing" (P2P) is a method of communication available to Internet users through the use of special software, which may be downloaded from the Internet. In general, P2P software allows a user to share files on a computer with other computer users running compatible P2P software. A user may obtain files by opening the P2P software on the user's computer and searching for files that are currently being shared on the network. A P2P file transfer is assisted by reference to the IP addresses of computers on the network: an IP address identifies the location of each P2P computer and makes it possible for data to be transferred between computers. One aspect of P2P file sharing is that multiple files may be downloaded at the same time. Another aspect of P2P file sharing is that, when downloading a file, portions of that file may come from multiple other users on the network to facilitate faster downloading.

i. When a user wishes to share a file, the user adds the file to shared library files (either by downloading a file from another user or by copying any file into the shared directory), and the file's hash value is recorded by the P2P software.

The hash value is independent of the file name; that is, any change in the name of the file will not change the hash value.

ii. Third party software is available to identify the IP address of a P2P computer that is sending a file. Such software monitors and logs Internet and local network traffic.

o. "VPN" means a virtual private network. A VPN extends a private network across public networks like the Internet. It enables a host computer to send and receive data across shared or public networks as if they were an integral part of a private network with all the functionality, security, and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two. The VPN connection across the Internet is technically a wide area network (WAN) link between the sites. From a user perspective, the extended network resources are accessed in the same way as resources available from a private network-hence the name "virtual private network." The communication between two VPN endpoints is encrypted and usually cannot be intercepted by law enforcement.

p. "Encryption" is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it but authorized parties can. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any unintended party that

can see the ciphertext should not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption algorithm that usually requires a secret decryption key, to which adversaries do not have access.

q. "Malware," short for malicious (or malevolent) software, is software used or programmed by attackers to disrupt computer operations, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. Malware is a general term used to refer to a variety of forms of hostile or intrusive software.

Computers, Electronic/Magnetic Storage, and Forensic Analysis

65. As described above and in Attachment B, this application seeks permission to search for evidence, fruits, contraband, instrumentalities, and information that might be found on the locations to be searched, in whatever form they are found. One form in which such items might be found is data stored on one or more digital devices. Such devices are defined above and include any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic

tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Thus, the warrant applied for would authorize the seizure of digital devices or, potentially, the copying of stored information, all under Rule 41(e)(2)(B). Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that, if digital devices are found on the PREMISES, there is probable cause to believe that the items described in Attachment B will be stored in the Device(s) for at least the following reasons:

a. Individuals who engage in criminal activity, including documenting illegal activity, communicating with co-conspirators online; storing on digital devices, like the Device(s), documents, photos, videos, and records relating to their illegal activity, which can include logs of online chats with co-conspirators; email correspondence; text or other "Short Message Service" ("SMS") messages; contact information of co-conspirators, including telephone numbers, email addresses, identifiers for instant messaging and social medial accounts.

a. Individuals who engage in the foregoing criminal activity, in the event that they change digital devices, will often "back up" or transfer files from their old digital devices to that of their new digital devices, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.

b. Digital device files, or remnants of such files, can be recovered months or even many years after they have been downloaded onto the medium or device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years

at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person "deletes" a file on a digital device such as a home computer, a smart phone, or a memory card, the data contained in the file does not actually disappear; rather, that data remains on the storage medium and within the device unless and until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the digital device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve "residue" of an electronic file from a digital device depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer, smart phone, or other digital device habits.

66. As further described in Attachment B, this application seeks permission to locate not only electronic evidence or information that might serve as direct evidence of the crimes described in this affidavit, but also for forensic electronic evidence or information that establishes how the digital device(s) were used, the purpose of their use, who used them (or did not), and when. Based on my knowledge, training, and experience, as well as information related to me by

agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit there is probable cause to believe that this forensic electronic evidence and information will be in any of the Device(s) at issue here because:

c. Although some of the records called for by this warrant might be found in the form of user-generated documents or records (such as word processing, picture, movie, or texting files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials contained on the digital device(s) are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive, flash drive, memory card, or other electronic storage media image as a whole. Digital data stored in the Device(s), not currently associated with any file, can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on a hard drive that show what tasks and processes on a digital device were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on a hard drive, flash drive, memory card, or memory chip that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times a computer, smart phone, or other digital device was

in use. Computer, smart phone, and other digital device file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

d. Forensic evidence on a digital device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, chats, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time, and potentially who did not.

e. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how such digital devices were used, the purpose of their use, who used them, and when.

f. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital device evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on digital devices is evidence may depend

on other information stored on the devices and the application of knowledge about how the devices behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

g. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on the device. For example, the presence or absence of counter-forensic programs, anti-virus programs (and associated data), and malware may be relevant to establishing the user's intent and the identity of the user.

h. I know that when an individual uses a digital device to plan and document illegal activity, the individual's device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The digital device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a digital device used to commit a crime of this type may contain data that is evidence of how the digital device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense and the identities of those perpetrating it.

Methods to be Used to Search Digital Devices

67. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital

devices, I know that:

a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time, in part because there are so many types of digital devices and software programs in use today. Digital devices – whether, for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. Recovery of "residue" of electronic files from digital devices also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is often essential to conducting a complete and accurate analysis of data stored on digital devices.

c. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of

particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregable from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment, and can require substantial time.

d. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear as though the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting "keyword" search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format ("PDF"), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text

format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography, a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband, or instrumentalities of a crime.

e. Analyzing the contents of mobile devices, including tablets, can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as "AES-256 encryption" to secure and encrypt the operating system and application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most

smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, "Hide It Pro," disguises itself as an audio application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

f. Based on all of the foregoing, I respectfully submit that searching any digital device for the information, records, or evidence pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the devices. In light of these difficulties, I request permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this warrant.

68. The volume of data stored on many digital devices will typically be so large that it will be extremely impractical to search for data during the physical search of the premises.

a. Therefore, in searching for information, records, or evidence, further described in Attachment B, law enforcement personnel executing this search warrant will employ the following procedures:

1. Upon securing the locations to be searched, law enforcement personnel will, consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, seize any digital devices (that is, the Device(s)), within the scope of this warrant as defined above, deemed capable of containing the information, records, or evidence described in Attachment B and transport these items to an appropriate law enforcement laboratory or similar facility for review. For all the reasons described above, it would not be feasible to conduct a complete, safe, and appropriate search of any such digital devices at the PREMISES, BUSINESS, and VEHICLE. The digital devices, and/or any digital images thereof created by law enforcement sometimes with the aid of a technical expert, in an appropriate setting, in aid of the examination and review, will be examined and reviewed in order to extract and seize the information, records, or evidence described in Attachment B.

2. The analysis of the contents of the digital devices may entail any or all of various forensic techniques as circumstances warrant. Such techniques may include, but shall not be limited to, surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); conducting a file-by-file review by "opening," reviewing, or reading the images or first few "pages" of such files in order to determine their precise contents; "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic "keyword" searches

through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

3. In searching the digital devices, the forensic examiners may examine as much of the contents of the digital devices as deemed necessary to make a determination as to whether the contents fall within the items to be seized as set forth in Attachment B. In addition, the forensic examiners may search for and attempt to recover "deleted," "hidden," or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching the contents of the seized digital devices will be specifically chosen to identify the specific items to be seized under this warrant.

Biometric Access to Device(s)

69. This warrant permits law enforcement agents to obtain from the person of Elliot BISHAI and Elias IRIZARRY (but not any other individuals present at the time of execution of the warrant) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s) requiring such biometic access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person(s)' physical biometric characteristics will unlock the Device(s). The grounds for this request are as follows:

70. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

71. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

72. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face.

Facial recognition features found on devices produced by other manufacturers (such as Apple's "Face ID") have different names but operate similarly to Trusted Face.

73. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

74. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

75. As discussed in this Affidavit, I have reason to believe that one or more digital devices, the Device(s), will be found during the search. The passcode or password that would unlock the Device(s) subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data

contained within the Device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

76. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

77. Due to the foregoing, if law enforcement personnel encounter any Device(s) that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to obtain from the aforementioned person(s) the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s), including to (1) press or swipe the fingers (including thumbs) of the aforementioned person(s) to the fingerprint

scanner of the Device(s) found at the locations to be searched; (2) hold the Device(s) found at the locations to be searched in front of the face of the aforementioned person(s) to activate the facial recognition feature; and/or (3) hold the Device(s) found at the locations to be searched in front of the face of the aforementioned person(s) to activate the iris recognition feature, for the purpose of attempting to unlock the Device(s) in order to search the contents as authorized by this warrant.

78. The proposed warrant does not authorize law enforcement to require that the aforementioned person(s) state or otherwise provide the password, or identify specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the Device(s). Nor does the proposed warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person(s) to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person(s) would be permitted under the proposed warrant. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned person(s) for the password to any Device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Device(s), the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

AUTHORIZATION TO SEARCH AT ANY TIME OF THE DAY OR NIGHT

79. Your affiant requests that the warrants be authorized to be executed at any time day or night for the following reasons. Law enforcement intends to arrest TANIOS on an outstanding warrant the evening of March 14, 2021, likely after 10:00 p.m. Law enforcement believes there is a great likelihood that once TANIOS is in custody friends, family members, or co-conspirators may seek to destroy evidence at the PREMISES, BUSINESS, or in the VEHICLE. Therefore, your affiant seeks authorization to execute the warrant execution past 10:00 p.m. on March 14, 2021. It is anticipated that law enforcement personnel will attempt to image or copy digital information from certain servers on the PREMISES, BUSINESS, and VEHICLE rather than remove those servers from the premises. Such onsite imaging or copying will minimize disruptions to the use of those servers.

80. From my training and experience, I know that imaging or copying information from servers on the PREMISES, BUSINESS, and VEHICLE can be substantially delayed by various factors which cannot be ascertained or sometimes even anticipated until the actual execution of the warrant. There may, for example, be no system administrator available, willing, or able to assist law enforcement personnel to narrow the search by identifying the virtual or dedicated server(s) on the PREMISES, BUSINESS, and VEHICLE or the server folders, containing information within the scope of the warrant. There may be terabytes or even petabytes of information to be copied. The network architecture of the servers on the PREMISES, BUSINESS, and VEHICLE or the configuration of the server hardware may affect and delay data transfer

speeds. Data encryption and password protections may also significantly delay imaging or copying as law enforcement personnel seek to identify necessary passwords without which imaging or copying on the PREMISES would likely be unachievable. Under some circumstances, data downloads can be interrupted by network or hardware malfunctions or other network or hardware attributes which often necessitates restarting the data downloads from the beginning.

81. For all of the foregoing reasons, I respectfully submit that good cause exists, pursuant to Fed. R. Crim. P. 41(e)(2)(A)(ii), for authorization to execute the search warrant at any time of the day or night. Law enforcement personnel will commence executing the warrant as near to 6:00 a.m. as practicable. However, given the myriad factors that that may prevent completion of the search and seizure by 10:00 p.m., including those described above, I request authorization to continue the warrant execution past 10:00 p.m., if necessary, until completion of the warrant execution. Suspending the execution at 10:00 p.m. until 6:00 a.m. could compromise data downloads in progress, render stored data subject to alteration or deletion, require securing the PREMISES during the intervening hours, and prolong the disruption of access to, and use of, the PREMISES and the digital devices being searched.

CONCLUSION

81. I submit that this affidavit supports probable cause for a warrant to search the PREMISES, BUSINESS, and VEHICLE described in Attachment A and to seize the items described in Attachment B.

Respectfully submitted,

Riley Palmertree
Special Agent
Federal Bureau of Investigation

Subscribed and sworn pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) on March 14, 2021. by phone

MICHAEL JOHN ALOI,
UNITED STATES MAGISTRATE JUDGE